IN THE CLAIMS:

Please cancel claims 1-23 without prejudice or disclaimer, and substitute new claims 24-46 therefor as follows:

Claims 1-23 (Cancelled).

24. (New) A method for the cipher controlled exploitation of data resources stored in a database associated with a computer system, comprising the steps of:

providing a subscriber identity module carrying at least one security algorithm;

producing a cipher key via said at least one security algorithm; and

using said cipher key for protecting said data resources.

25. (New) The method according to claim 24, wherein said step of using said cipher key for protecting said data resources comprises the steps of:

encrypting said data resources by means of said cipher key;

storing said encrypted data resources in said database associated with said computer system;

retrieving said encrypted data resources from said database; and

decrypting said encrypted data resources by means of said cipher key.

26. (New) The method according to claim 24, wherein said step of producing a cipher key comprises the steps of:

generating at least one random value;

subjecting said at least one random value to said at least one security algorithm to generate at least one session key; and

processing said at least one session key via a mixer function to produce said at least one cipher key.

27. (New) The method according to claim 26, comprising the steps of:

generating at least two random values;

subjecting said at least two random values to said at least one security algorithm to generate at least two session keys; and

combining said at least two session keys via a mixer function to produce said at least one cipher key.

28. (New) The method according to claim 26, wherein said mixer function comprises a hash function.

29. (New) The method according to claim 26, comprising the step of inserting in said mixer function a user specific secret unrelated to said subscriber identity module security algorithm, whereby said cipher key is unpredictable even based on knowledge of said security algorithm carried in said subscriber identity module.

30. (New) The method according to claim 24, comprising the step of selecting said data resources from user sensitive data or user credentials.

31. (New) The method according to claim 30, wherein said step of using said cipher key for protecting said data resources comprises the step of encrypting by means of said cipher key, said user sensitive data or said user credentials from plain text into an encrypted format.

32. (New) The method according to claim 31, wherein said step of using said cipher key for protecting said data resources comprises the step of decrypting by means

of said cipher key said user sensitive data or said user credentials from an encrypted format into plain text.

33. (New) The method according to claim 31, wherein said user sensitive data or said user credentials in encrypted format have a cryptographic header associated therewith.

34. (New) The method according to claim 33, wherein said cryptographic header comprises an identifier of said subscriber identity module and a cryptographic checksum based on said cipher key, said cryptographic checksum being used for detecting any unauthorized modifications of said encrypted format.

35. (New) The method according to claim 30, wherein said data resources are user credentials, said database associated with said computer system is a remote database and said data resources based on said user credentials are stored in said remote database in an encrypted format.

36. (New) The method according to claim 35, comprising the step of establishing a relationship between said user credentials stored in said encrypted format in said remote database and a corresponding user subscriber identity module.

37. (New) The method according to claim 36, wherein said relationship is established by means of an identifier of said subscriber identity module.

38. (New) The method according to claim 37, comprising the step of using said identifier for searching within said remote database to permit said user exploitation of said user credentials.

39. (New) A system for the cipher-controlled exploitation of data resources, comprising:

at least a subscriber identity module carrying at least one security algorithm;

at least a computer system comprising at least one processing module, said processing module being interfaced with said subscriber identity module to generate at least one cipher key via said at least one security algorithm and being configured to protect via said cipher key said data resources; and

a database associated with said computer system for storing said data resources protected by said cipher key.

40. (New) The system according to claim 39, wherein said at least one processing module is configured for:

encrypting said data resources by means of said cipher key;

storing said encrypted data resources in said database associated with said computer system;

retrieving said encrypted data resources from said database; and

decrypting said encrypted data resources by means of said cipher key.

41. (New) The system according to claim 39, wherein said database is included in said computer system.

42. (New) The system according to claim 39, wherein said database is remote from said computer system.

43. (New) The system according to claim 39, wherein said processing module is interfaced with said subscriber identity module via a smart card reader or a Bluetooth mobile terminal or an IrDA mobile terminal or a mobile terminal through a cable.

44. (New) The system according to claim 39, wherein said computer system comprises a personal computer or a notebook or a laptop or a PDA, or a smart phone.

45. (New) A communication network comprising a system according to claim 39.

46. (New) A computer program product loadable in the memory of at least one computer and comprising software code portions capable of performing the method of claim 24.